CHAPTER 4 — INFORMATION TECHNOLOGY

ARTICLE 1 — INFORMATION TECHNOLOGY DEFINITIONS AND ACRONYMS

Revised July, 18, 2013

41010.1 Policy

The Director, Enterprise Information Services (EIS) and Executive Management of the California Department of Corrections and Rehabilitation (CDCR) recognize Information Technology (IT) as an indispensable tool of modern government. Therefore, it is the policy of the Director to support and promote the departmental use of innovative information technologies in order to increase worker productivity, improve departmental services, and strengthen the overall effectiveness of management, while saving money and reducing the overall cost of government. The definitions and acronyms contained here ensure the consistent use of IT definitions and acronyms throughout the Department Operations Manual (DOM) Chapter 4 – Information Technology.

41010.2 Purpose

The purpose of the Department's IT Definitions and Acronyms policy is to ensure that proven management methods for the guidance and control of planning, acquisition, development, operation, maintenance, and evaluation of information management applications are established in a manner that provides for the most efficient, effective, and economical use of the Department's resources for IT.

41010.3 Definitions

-A-

Access

Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

Access Authorization

The granting of permission to execute a set of operations in a computer system.

Access Control

The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances).

Access Management Group

A group that is responsible for access permissions granted to CDCR's Information Assets, including the CDCR Network, and departmental applications and databases.

Accountability

The state of being liable, responsible and answerable.

AISO

Agency Information Security Office - Provides information security recommendations, guidance, and authority.

AMS

Application Maintenance and Support - Provides IT business application development, maintenance and support services spanning across all CDCR divisions, including adult and juvenile offenders, parole operations, and administration.

Application Disaster Recovery Plan

A plan devised to process a computer application (application) after is has been distrupted for some period of time.

Asset

Anything (tangible or intangible) that has value to CDCR.

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. To access most technology services you must provide such proof of identity. In private and public computer networks (including the Internet), authentication is commonly used by requiring login passwords or passphrases; knowledge of such is assumed to guarantee that the user is authentic. Thus, when you are asked to "authenticate" to a system, it usually means that you enter your username and/or password for that system.

Authorization

In computing systems, authorization is the process of determining which permissions a person or system is supposed to have. In multi-user computing systems, a system administrator defines which users are allowed access to the system, as well as the level of privileges they are eligible to access (e.g., access to file directories, hours of access, amount of allocated storage space). Authorization can be seen as both the preliminary setting of permissions by a system administrator, and the actual checking of the permission values when a user obtains access. Authorization is usually preceded by authentication.

Availability

Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

-B-

Back-up

A process by which data is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted.

BIS

Business Information System - A fully implemented automated business management system that creates, tracks and reports all of the Department's business transactions.

Blog

A web site containing frequent publications of personal thoughts and web links, coined from the words weblog, maintained for the purpose of commentary, or other material such as graphics or video.

BPH

Board of Parole Hearings - Conducts parole consideration; rescission, parole, revocation, and parole progress hearings for adult inmates and parolees.

Business Continuity Management Program

An ongoing governance process supported by senior management and resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products/services through exercising, rehearsal, testing, training, and maintenance.

Business Continuity Plan (BCP)

A plan that documents arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical business functions after an interruption.

-C-

CALPIA

California Prison Industry Authority - A State-operated agency that provides productive work assignments for offenders in California's adult correctional institutions. CALPIA operates more than 60 service, manufacturing, and agricultural industries at prisons throughout California.

CAS

Corrections Application Solutions - Develops and maintains applications and systems used by divisions and programs throughout CDCR to support statewide offender, parole, and juvenile operations.

CCHCS

California Correctional Health Care Services - A department under federal receivership responsible for providing constitutionally adequate medical care to patient-inmates of the CDCR within a delivery system the state can successfully manage and sustain.

CDCR Network

The system of telecommunication devices, workstations, servers, and peripherals used to provide inter- and intra-facility connectivity that enable CDCR employees to access information assets and electronic communications. The CDCR Network is managed by the CDCR Enterprise Information Services (EIS) division and the Office of Technology Services (OTech).

Chain E-mail or Letter

E-mail sent to successive people. Typically the email contains directions for the recipient to forward the email to multiple people. The contents usually contain promises of good luck for the recipient or money if the directions are followed.

Classification

The assignment of information, including a document, to a category on the basis of its sensitivity concerning disclosure, modification, or destruction.

Client (User)

The individual or organization that utilizes a product.

Component

A component is defined in SAM § 5013 as any individually identified piece of hardware, such as the mainframe, tape drive, disk drive, power supply unit, controller, punch, reader, printer, modem, CRT, keyboard, remote device, and the like.

Computer Contaminant

Any set of computer instructions that, outside the intent and without the permission of the owner of such information, is designed to modify, damage, or destroy a computer, system, or network, or to record or transmit information within a computer, system, or network. Such contaminants include, but are not limited to, the group of self-replicating or self-propagating computer instructions commonly termed viruses, Trojans, and worms which are designed to affect computer programs or data, consume computer resources, modify, destroy, record or transmit data, or otherwise usurp the normal operation of the computer, system, or network.

Computer Network

Any system that provides communication among one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

Computer Program or Software

A set of instructions, or statements or related data, that when executed in actual or modified form cause a computer, system, or network to perform specified functions.

Computer Security

The technological safeguards and managerial procedures that can be applied to computer hardware, programs, data, and facilities to ensure the availability, integrity, and confidentiality of computer-based resources. This can also include assurance that intended functions are performed as planned.

Computer Services

Includes, but is not limited to, computer time, data processing, storage functions, other uses of a computer, system, or network.

Computer System

A device or collection of devices, including support devices but excluding calculators that are not programmable and not capable of being used in conjunction with external files, one or more of which contains computer programs, electronic instructions, input data, and output data, and which performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

Computer-Based Tools

Software or computer programs that improve or enable a user's ability to configure and manage IT components.

Confidential Information

Information maintained by State agencies that is exempt from disclosure under provisions of the California Public Records Act (PRA) (GC § 6250 et seq.) or other applicable state or federal laws. All inmate, parolee, ward, and employee information that has not been explicitly defined as public information in §3261.2 of Title 15 should be treated as Confidential Information.

Confidentiality

Assurance that information is shared only among authorized persons or organizations. Breaches of confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating other data. The classification of the information should determine its confidentiality and the appropriate safeguards.

Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)

Enables CDCR to perform needs assessments and follow adult offenders from their intake at the reception centers through the completion of their parole supervision requirements.

Cost Thresholds

Cost thresholds are the set dollar amounts assigned to agencies based on their size and past experiences with Department delegations can be found at:

http://www.cio.ca.gov/Contact_Us/staff_assignments.html

CPAT

California Parole Apprehension Team – Enhances public safety through parole intervention and parolee-at-large apprehension.

Critical Application

An application that is so important to the Department that its loss or unavailability is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or Department employees, the fiscal or legal integrity of operations, or the continuation of essential programs.

CTA

California Technology Agency – State of California's IT control agency.

Custodian of Information

An employee or organizational unit (such as a data center or information processing facility) acting as caretaker of an automated file or database.

-D-

DART

Desktop Advanced Research Team – Provides system level operational support of all end-point devices.

Data

A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automated means.

Data Classification

Data Classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, sorted, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled/secured and is indicative of its value in terms of Business Assets. The classification of data and documents is essential to differentiate between that which is of little (if any) value, and that which is highly sensitive and confidential. The classification of data helps determine what baseline security controls are appropriate.

Data Processing Equipment

Computers, network components, and other devices that facilitate, enable, or depend upon data communications. Network devices such as, but not limited to, routers, hubs, wires, and servers are data processing equipment.

Data Processing Systems

A system, including computer systems and associated personnel, that performs input, processing, storage, output, and control functions to accomplish a sequence of operations on data.

Data Security

Protecting data from unauthorized access, modification, destruction, or disclosure.

Data Transmission

The conveying of data from one functional unit to one or more additional functional units through the transmission of signals by wire, radio, light beam, or any other electromagnetic means.

DEC

Disability Effective Communications System - An IT program created and maintained by EIS that ensures that inmate and parolee due process rights are recognized by identifying and accommodating their disabilities and effective communication special needs.

Decentralized Applications

Systems that run on more than one computer in geographically separated locations. The term also refers to systems that are not supported by a single organization, such as EIS.

Defect

A variance from specifications/standards or an attribute/function not contained in the software requirements specifications.

Denial of Service

An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

Deputy Director Operations

Responsible for all aspects of EIS's day-to-day operations.

Development

Activities or costs associated with the analysis, design, programming, staff training, data conversion, acquisition, and implementation of new IT applications.

Disaster Recovery Operation

The act of recovering from the effects of a disaster or disruption to a computer facility, and the preplanned restoration of facility capabilities.

Disaster

A human or natural occurrence causing destruction and distress, after which a business is deemed unable to function.

Disaster Recovery

The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.

DRP

Disaster Recovery Plan - The management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort. Usually refers to the technology recovery effort. This is a component of the Business Continuity Plan.

Documentation

Information about how specific applications are constructed, maintained, and used. It includes, but is not limited to, system and program design specifications, record formats, report layouts, program source and object code, job control language specifications, run instructions, key entry instructions, and data definitions.

DRD Tracker

Discharge Review State Tracker - Creates a calendar-based event driven solution which allows field agents and case records staff to determine when a parolee is due for a Discharge Review.

-E-

E-mail

Written communication transmitted electronically using computers connected to network(s). Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to an email server, for as long as it takes to send or receive messages.

EdCATS

Education Classroom Attendance Tracking System - Allows teachers to log academic and vocational classroom hours and track milestones achieved by students while attending those classes.

EIS

Enterprise Information Services - A division of CDCR responsible for the enterprise-wide execution of all IT systems and services.

Electronic Data Processing (EDP) Equipment

EDP equipment is defined as:

• Central processing units and all related features and peripheral units, including processor storage, console devices, channel devices, etc.

• Minicomputers, microcomputers, personal computers, and all peripheral units associated with such computers.

• Special purpose systems including word processing, magnetic ink character recognition, optical character recognition, photocomposition, typesetting, and electronic bookkeeping.

• Communications devices used for data transmission such as modems, data sets, multiplexors, concentrators, switches, local area networks, private branch exchanges, network control equipment, and microwave or satellite communications systems.

• Input-output (peripheral) units (off-line or on-line) including: terminals, card readers, optical character readers, magnetic tape units, mass storage devices, card punches, printers, computer output to microfilm converters, video display units, data entry devices, FAXs, teleprinters, plotters, or any device used as a terminal to a computer, and control units for such devices.

Encryption

Data encryption is a means of scrambling or ciphering the data so that it can be read only by the recipient - the person(s) holding the 'key' – a password of some sort. Without the 'key,' the ciphered data cannot be opened and read.

Enterprise Architecture (EA)

The CDCR unit responsible for managing CDCR's enterprise architecture program, a strategic practice for maintaining the IT architecture portfolio to facilitate more informed and effective IT decisionmaking, both strategically and operationally. This includes, but is not limited to, the Business, Application, Information/Data, Technical, and Security Architecture domains.

eOMIS

Electronic Offender Management Information System - A real-time application that increases the availability of accurate and complete offender information so CDCR can more efficiently manage inmates.

ERMS

Electronic Records Management System - A document management system that provides a digitally scanned and uploaded central records repository.

EWACS

Enterprise Web and Collaboration Solutions - Provides web application development, operational support, and end user support for the enterprise. Develops public and internal facing web and client-based applications that meet various business needs.

-F-

Failure

Inability of a product or service to perform its required functions within previously established limits.

FIS

Field Information System – Documents all contacts by parole agents with juvenile offenders.

Forwarded E-mail

E-mail resent from an internal network to an outside point, whether internal or external to CDCR.

-G-

Guideline

A description that clarifies what should be done and how to achieve the objectives set out in policies.

-H-

Handheld Computer

Synonym for Personal Digital Assistant.

Hardening

A defense strategy to protect against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls.

Hardware

The physical equipment or machinery (computers, terminals, printers, disc drives, etc.) used in IT systems.

HAWI

Holds and Warrants Interface - Easily accesses parolee information to automate the issuance of holds and warrants.

High Risk Confidential Information (HRCI)

Non-public information that if disclosed could result in a significant harm (including financial, legal, risk to life and safety or reputational damage) to the CDCR or individual(s). Examples of HRCI include, but are not limited to, information such as the following:

- Personally identifiable information such as person's name in conjunction with the person's Social Security Number, credit or debit card information, individual financial account, driver's license number, state ID number, passport number, or a name in conjunction with biometric information;
- Personal health information such as any information about health status, provisions of health care, or payment for health care information as protected under HIPAA;
- Correctional Offender Record Information
- Information that if disclosed would "reveal vulnerabilities to, or otherwise increase, the potential for an attack on an IT system of a public agency." Examples include, but are not limited to, firewall and router configurations, server names, IP addresses, and other system configuration details;
- Any documentation of information which contains information or data within any Gang Database.
- Records of investigations, intelligence information, or security procedures. This includes, but is not limited to, information identifying confidential informants.

-I-

Information Assets

All categories of information existing in any form, including electronic or hard copy that is stored, used, or created by CDCR and have value to the organization.

Information Governance

The process of official enterprise-level decisionmaking for CDCR information standards to ensure the effective, efficient, and secure use of CDCR information. This includes officially making and adopting Data Classification decisions for CDCR information.

Information Integrity

The condition in which information or programs are preserved for their intended purpose, including the accuracy and completeness of information systems and the data maintenance within those systems.

Information Owner

Group(s) or person(s) responsible for individual and/or collective decision-making regarding specific CDCR Information Assets. This includes decision-making regarding the appropriate use, access, controls, and Data Classifications for those Information Assets.

Information Processing

The systematic performance of operations upon data such as handling, merging, sorting, and computing; synonymous with data processing systems.

Information Security

The protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information exists in many forms: printed or written on paper, stored electronically, transmitted by post or electronic means, on films, and spoken.

Information Security Incident

An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information Security Standards and Guidelines (ISSG)

Compilation of the standards and guidelines comprising CDCR's program to ensure the protection and security of information as*sets.

Information Technology

All computerized and auxiliary automated information handling, including: Systems design and analysis; conversion of data; computer programming; information storage and retrieval; voice, video, and data communications; requisite system controls; simulation; and, all related interactions between people and machines.

Input-Output Unit/Device

The equipment used to communicate with a computer; commonly termed I/O (Input/Output).

Instant Message (IM)

A type of communications service that enables a user to exchange text messages in real time among two or more individuals logged into a particular instant messaging system from a computer workstation.

Integrity

As it pertains to data, is the assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose. The integrity is not only whether the data is correct, but also whether it can be trusted and relied upon.

Internet

The World Wide Web (WWW), consisting of a network of networks.

Intranet

A term that refers to a closed network of networks. In the context of CDCR, it refers to the web portal used for hosting information and documents for internal CDCR users only.

IS

Infrastructure Services - Creates, maintains, and supports all enterprise data activity necessary to facilitate CDCR's current and future business needs as well as provide ongoing operations, production implementation, and control in a secure manner.

ISC

Information Security Coordinator - Each entity's ISC is responsible for ensuring that applicable CDCR IT security policies and procedures are followed.

IT CSFO

IT Customer Service and Field Operations - Provides quality service, guidance and direction to customers in order to support their business needs by implementing cost-effective, innovative technologies and adopting operational IT best practices and standards.

ITPSP

IT Policy and Strategic Planning - Drives enterprise IT planning efforts necessary to support the Agency's mission and future investments while ensuring compliance with national, State and local mandates.

-J-

-K-

-L-

Law Enforcement Automated Data System (LEADS)

Parole LEADS is a web-based computer system that provides local California law enforcement agencies with information on CDCR parolees.

Life Cycle

The anticipated length of time that the IT system or application can be expected to be efficient and cost-effective and can continue to meet the agency's programmatic requirements; synonymous with operational life of a system.

LINX

Link Investigation and Network Cross-Reference - Centralized web-based application that contains inmate gang affiliations and validation for adult offenders.

Local Area Network

A Local Area Network (LAN) is a computer network consisting of telecommunications devices such as routers, hubs, switches, firewalls, and computers such as workstations, servers, and peripheral devices.

LSTS

Lifer Scheduling and Tracking System - Supports the inmates sentenced to life parole suitability hearing process.

-M-

Mainframe

Refers to large computers typically housed in a data center environment and running legacy systems. Mainframe computers have security components, such as Resource Access Management Systems, integrated into the operating system and can support many hundreds of users simultaneously.

Malicious Software

Malicious software, or malware, is any set of computer instructions that, outside the intent and without the permission of the owner of such information, is designed to modify, damage, or destroy a computer, system, or network, or to record or transmit information within a computer, system, or network. Such contaminants include, but are not limited to, the group of self-replicating or self-propagating computer instructions commonly termed viruses. Trojan Horses and worms are designed to affect computer programs or data, consume computer resources, modify, destroy, record, or transmit data, or otherwise usurp the normal operation of the computer, computer system, or computer network. Malware includes computer viruses, computer worms, Trojan Horses, most root kits, spyware, dishonest adware and other malicious or unwanted software.

MDO

Mentally Disorder Offender - Database that tracks MDO holds, creates hearing schedules, generates confirmation letters for evaluators and attorneys, and tracks MDO cases.

Mission-Critical Applications

Applications defined by CDCR that support business activities or processes that cannot be interrupted or unavailable for the Recovery Time Objective (RTO) defined by the agency without significantly jeopardizing the organization.

-N-

Need-to-Know

Refers to a person having both a legitimate right and a reason to obtain information.

NIST

National Institute of Standards and Technology - A measurement standards laboratory which is a non-regulatory agency. NIST promotes innovation and industrial competitiveness by advancing measurement science, standards, and technology.

-O-

OBITS

Offender Based Information Tracking System - Mission critical master record for all juvenile offender activity that feeds information into multiple systems.

One-Time Costs

Costs occurring only once that are associated with the analysis, design, programming, staff training, data conversion, acquisition, and implementation of new IT applications.

Operational Life

See Life Cycle.

Operations

Activities or costs associated with the continued use of IT applications. Operations include personnel associated with computer operations, including network operations, job control, scheduling, and key entry. It also includes the costs of computer time and other resources needed for processing. See SAM Section 4819.2.

OTech

Office of Technology Services - Provides IT services to many state, county, federal and local government entities throughout California.

Owner of Information

See Information Owner.

-P-

PACATS

Parolee Automated Cash Assistance Tracking System - Tracks cash assistance provided to parolees throughout the state, separated by assistance type.

PAL Trax

Parolee At Large Tracking System -Tracks CPAT agent caseloads.

Parole-LEADS

See Law Enforcement Automated Data System.

Personal Digital Assistant (PDA)

Palm-sized computer that syncs with a computer workstation and allows users to refer to information from the workstation without having to print it out. Schedules, e-mails, documents, and spreadsheets as well as reference material such as dictionaries and phone lists can be stored and accessed as needed on the device. PDAs often are capable of wireless connectivity with LANs and the Internet.

Personally Identifiable Information

Personally Identifiable Information (PII) is the manifestation of an individual's first name or first initial and last name, in combination with one or more of the following:

- Social Security Number;
- Driver's license number;
- State issued ID card;
- Credit or debit card number in combination with any required security code or password that could permit access to an individual's financial account;
- Medical information, history, mental or physical condition, treatment or diagnosis by a health care professional;
- Health information, policy number or subscriber ID, unique identifier, or any information in an application and claims history, including any appeals records.

Physical Security

The measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against unauthorized access, damage, and theft.

Post Implementation Evaluation Report (PIER)

The review of a computer, computer system, or computer network that has been in operation for at least six months and no longer than two years for the purpose of matching the requirements of the system against what has been produced so as to ensure that stated requirements have been met.

Policy

Overall intention and direction as formally expressed by management.

PPP

Parole Planning and Placement - Obtains and utilizes information about offenders in order to develop and implement effective and specific reentry plans that maximize a parolee's opportunity to successfully reintegrate into the community.

PPPMA

Policy/Planning, Project Management and Acquisitions is the EIS unit responsible for EA, PPRM, QPAC, and ITPSP.

PPRM

Portfolio, Project and Resource Management is the EIS unit that improves the management of IT investments by utilizing project and portfolio managements tools; incorporating proven methodologies; and following best practice disciplines to assist in the identification, ranking, and justification of investments and the implementation of funded projects.

PRAS

Parole Restitution Application System - Tracks original court ordered restitution payments and balances.

Privacy

The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Process

The work activities that produce products, including the efforts of people and equipment.

Product

The output of a process, including the goods and services produced by individuals and the organization.

Production Application

A computer-based process that stores, manipulates, or reports departmental information.

Program

In the IT field, a program is the set of instructions by which a computer operates to accomplish a specific task.

Program Application Manager

Department supervisory and management staff responsible for managing or supervising employees' use of an automated file or database.

Programming

Detailed design encompassing the actual development and writing of program units or modules.

Project

A planned sequence of tasks to respond to a problem or opportunity; an activity with a beginning and an end and containing a set of resources.

Proprietary Software

Software packages which are developed by independent vendors and marketed to users.

Protected Health Information

Individually identifiable information in electronic or physical form created, received, or maintained by health care organizations such as health care payers, providers, plans, and contractors. State laws require special precautions to protect from unauthorized use, access or disclosure.

Protected Personal Information

Information that identifies or describes an individual and must be protected from inappropriate access, use, or disclosure as defined in applicable state and federal laws.

Protecting Sensitive Information

Typically means providing for one or more of the following:

- Confidentiality – Disclosure of the information must be restricted to designated parties.
- Integrity – The information must be protected from errors or unauthorized modification.
- Availability – The information must be available within some given timeframe (i.e., protected against destruction). (NIST Computer System Laboratory CSL Bulletin 92-11.)

Public Information

Information maintained by State agencies that is not exempt from disclosure under the provisions of state or federal laws. Public Information is open to inspection by any person during normal business hours (PRA § 6253(a)).

-Q-

QPAC

Quality Project Authority and Compliance – Staff in EIS that advocates for CDCR’s IT projects to Control Agencies for the purpose of securing project authority and funding approval, as well as the project’s successful completion.

Quality

The extent to which a product meets the expectations and requirements of the user.

Quality Assurance (QA)

(1) A staff function designed to support line management in performing the Quality Control function. As such, QA identifies the processes (both good and bad) which affect quality, and is used to advise management of such effects. A management decision may then be necessary to ensure that QC techniques are implemented and maintained; and, (2) The function that uses measurement and analysis to continually improve processing, procedures, and standards so that management can be reasonably assured of their staff following such methods, procedures, and standards, as well as staff's ability to produce products which meet specified requirements.

Quality Control (QC)

(1) The collection of activities to ensure that defects are neither made nor implemented. While QA monitors the processes involved in the production cycle, QC is an integral part of work and is the responsibility of each employee; and,

(2) A line function used to measure quality associated with specific products or services. QC is the responsibility of each IT area, and it is the function responsible for the quality of the work being done within a specific area or for a specific project.

-R-

Recovery Point Objective (RPO)

The maximum amount of data loss an organization can sustain during an event.

Recovery Time Objective (RTO)

The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTOs are used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

Requirement

The specification(s) for satisfying a user need is associated with a standard by which the satisfaction of that need can be measured.

Resource Access Management Facility

An application within IBM-based computer systems that reviews logons, passwords, and permissions before permitting access to information.

Risk

In the context of information systems, the likelihood or probability that a loss of information assets or breach of security will occur.

Risk Analysis

The process of identifying the vulnerabilities and threats to an organization by assessing the critical functions necessary for an organization to continue business operations, and defining the controls in place to reduce organization exposure and evaluating the cost for such controls.

Risk Assessment

Overall process of risk analysis and risk evaluation.

Risk Evaluation

The process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk Management

The process of coordinating activities to direct and control the organization with regard to risk.

-S-

Sensitive Information

Information maintained by State agencies that requires special precautions to protect it from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either Public or Confidential. It is information that requires a higher than normal assurance of accuracy and completeness. The key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of financial transactions and regulatory actions.

Smartphone

A cellular telephone with built-in applications and Internet access. Smartphones provide digital voice service as well as text messaging, e-mail, Web browsing, still and video cameras, MP3 players, video viewing and often video calling. In addition to their built-in functions, smartphones can run a myriad of applications, turning the once single-minded cellphone into a mobile computer.

Software

Programs, procedures, rules, and any associated documentation pertaining to the operation of a system. (Contrast with hardware.)

Spam

Unauthorized and/or unsolicited electronic mass mailings.

Stakeholder

A person, group, organization, member, or system who affects or can be affected by an organization’s or system’s actions.

-T-

Threat

The potential cause of an unwanted incident, which may result in harm to a system or organization.

-U-

Unauthorized Disclosure

The intentional or unintentional disclosure of confidential information to people inside and/or outside the CDCR who do not have authorization predicated on a "need to know" basis.

Unit Testing

Testing performed on a single, stand-alone module or unit of code.

User Identification (ID)

The logon name an individual user to access a computer or network system.

User of Information

An individual having specific limited authority from the owner of information to view, change, add to, disseminate, or delete such information.

-V-

Validation

The process of comparing a product in any stage of its development with specified requirements to determine whether the correct product is being produced.

Virus

Small but insidious piece of programming code that attacks computer and network systems through contaminated (infected) data files, introduced into a system via email, portable storage media or the Internet. The code attaches itself to the target computer's operating system or other programs, and may automatically replicate itself to spread to other computers or networks.

Vulnerability

A weakness of an asset or group of assets that can be exploited by one or more threats.

-W-

Wide Area Network (WAN)

Two or more LANs connected together. A communications network that uses devices over telephone lines, fiber-optics, satellite dishes, or radio waves to span a larger geographic area that can be covered by a LAN.

Wireless

Referring to communications transmitted without wires, such as radio, microwave, or infrared.

Workstation

Any device commonly called a microcomputer, personal computer, or terminal used for processing, storing, or sending information.

Worm

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself.

WWW

An abbreviation for World Wide Web. See Internet**.**

-X-

-Y-

-Z-

41010.4 Revisions

The Director of EIS, or designee, shall be responsible for ensuring that the contents of this Article are kept current and accurate.

41010.5 References

GC §§ 6250 - 6265, and 11702 (a).

Title 15 § 3261.2

SAM §§ 4819.2, 5013, 5320.5

DOM §§ 52070.22, 52070.24

Health Insurance Portability and Accountability Act (HIPAA) of 1996

PC 13100-13104

PRA § 6254.19

PRA § 6254 (f)

California Senate Bill 1386

Confidentiality of Medical Information Act, California Civil Code Section 56 et seq.
Patients' Access to Health Records Act
California Health and Safety Code Sections 123100-123149.5